There's Something in the Air: What's on the Horizon in the Mobile Cyber Threat and Fraud Arena

An IBM® Company

Presented in partnership with

cellebrite
mobile data secured

1

Agenda

- Instructions and introduction
- Josh Work: *Analytic Approaches to Understanding Mobile Cyber Threats*
- Paul Henry*: Mobile Security Considerations for the Enterprise*
- Christopher Shin: *Cellebrite UFED Mobile Device Data Extraction*
- Brandt Heatherington: *i2 Cyber Solution Overview*
- Q&A

2

Polling Question #1

- What sector are you employed in?
  - Federal or National Government Law Enforcement
  - State or Local Law Enforcement
  - Intelligence Agency
  - Other government agency
  - Commercial enterprise

3

Joshua Work

- Chief Intelligence Analyst at iSIGHT Partners
- Directs cyber threat intelligence analysis in support of US government and private sector clients
- Previously performed a variety of intelligence roles throughout government and the private sector, including collection management, analysis, and operational assignments
- Supporting missions for Department of Homeland Security, Department of Defense counterterrorism, counterinsurgency, and information operations missions, as well as other assignments focused on complex transnational issues and asymmetric threats
- B.A. in History / Intelligence Studies from Mercyhurst College
- Master of Arts in Intelligence Studies at American Military University
- Studied chemical, biological, nuclear, and explosives issues for Weapons of Mass Destruction certification at the Uniformed Services University of Health Sciences
- Developed and taught intelligence studies courses in both government and academic settings since 2001, covering a range of subjects including intelligence collection, analytic tradecraft, targeting, open source intelligence, and cyber intelligence

4

Adversary interest in mobile

- Increasingly important platform for user's computing presence
  - Social media
    - Identity and trust
    - Online gaming and virtual / ludic currencies
  - Banking
    - Today: multifactor authentication, auction, shopping
    - Coming soon: Phone as "wallet", near field payments?
  - Telecom and the enterprise
    - Premium services
    - Confidentiality / Integrity / Availability
    - Geolocative privacy

5

Threats and rumours of threats

- Increasing security industry research interest
- Observed "ransomware" campaigns
- Observed premium call termination fraud
- Lawful intercept regulatory emphasis (India, UAE, Saudi Arabia, South Africa, others)
  - Service provider level installation of intercept applications, RIM BB
  - Potential abuse of lawful intercept functionality for criminal purposes
- Social engineering vectors for malicious code in App marketplaces
- Adversary attempts to acquire weaponized exploits targeting Apple iOS devices

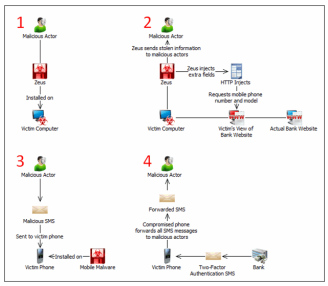
6

Case study: Adversary targeting mobile banking users

- July 2011, new detection of malware targeting Android operating system
  - Impersonating multifactor authentication application used by multiple financial institutions
  - Linked to ongoing Zeus credential collection malware campaigns
    - Previously targeting Symbian, Blackberry, Windows OS mobile devices

7

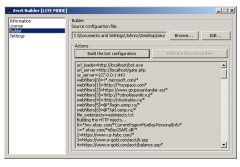
Zeus in the middle (ZITMO) TTP

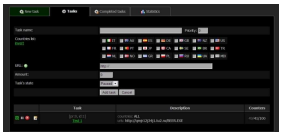


8

Zeus malware

- Credential collection Trojan family
  - Dominant underground marketshare
  - Replaced earlier generation malware such as PINCH, 311 Death/Haxdoor and Nuclear Grabber
  - Supports automated transactions, IM / Jabber notification, VNC / remote access to victim machines

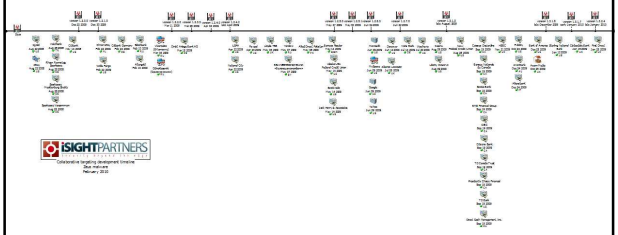




9

Zeus malware background

- Initial collaborative open source development model
  - Particularly notable in early collaborative targeting customization
    - Impacts banks, payment processors, brokerage firms, eCommerce firms, insurance firms



10

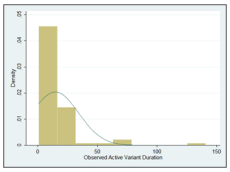
Zeus malware background

- Later shifted to underground commercialization
  - significant premium for new releases and continuing codebase updates
  - Commercialization of web inject and automation workflow
  - Increasing regional focus due to Western countermeasures
- Alleged monopoly claims unfounded
  - However, de-facto standardization of targeting and support infrastructure copied in later credential collection variants (Spyeye, Ice IX)

11

Zeus build variants

- Common version numbering
- Unique build number originally specific to purchaser
  - Believed approximately 2/3 of all builds detected
  - For every version, likely multiple undetected builds
- No honor among thieves
  - Certain variants widely proliferated in secondary markets
    - Version 1.4.2.1 notable
  - Occasionally deceptive version markings, to remarket older code at premium to unsophisticated buyers
- Source code leaks
  - Version 2.0.8.9, first released in August 2010, public leak since at least February 2011

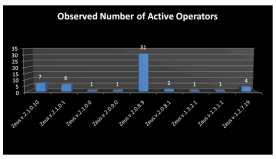


Active build versions exhibit a strong tendency to last only up 8.5 days. Undetected builds likely demonstrate a similar active duration.

12

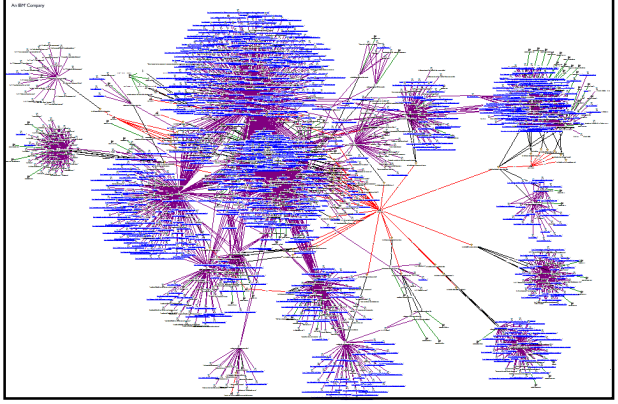
Understanding Zeus campaigns

- Zeus builds may also be characterized based on unique configuration and cryptographic features
- Zeus is a highly proliferated malware variant, so multiple operators (or operator groups) may use the same unique build
  - Data intensive analysis task, however identification of operator patterns is possible



Observed active Zeus operators using various versions from mid-May to early June 2011

13

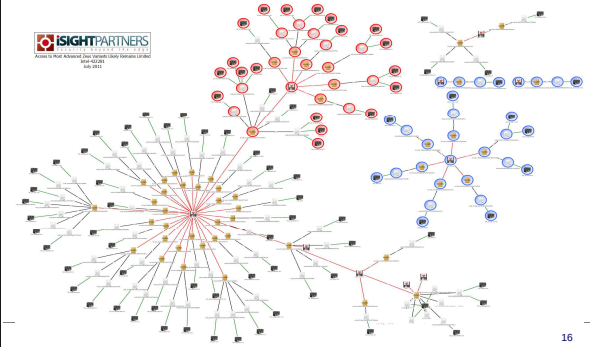


Mobile campaign

- Variant in July 2011 mobile threat incident identified as build 2.1.0.10
  - Sensitive source reporting indicates that this build variant is utilized by a continuing eCrime enterprise offering a private, illicit "software as a service" business model
  - Common infrastructure, but multiple operators
  - Multiple different distribution mechanisms, likely varying by operators / customers

15

Focusing on Zeus v2.1.0.10 (red)



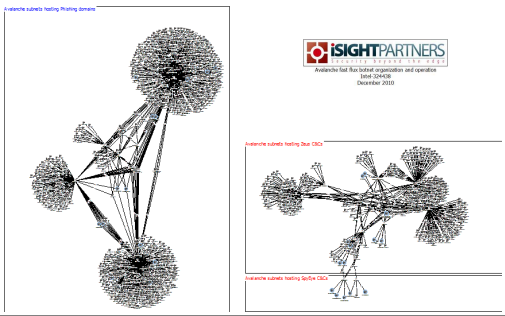
16

Campaign and hosting infrastructure

- Identified Zeus command & control linked to these ongoing campaigns was previously observed to be hosted on fast flux infrastructure
- This infrastructure was identified as part of the Avalanche botnet
  - Long-running botnet infrastructure, likely operated as a service by a continuing eCrime enterprise
  - Hosts multiple phishing and credential collection malware operations
  - Again, data intensive analysis task to understand these operations
    - However, operational patterns are identifiable
    - Indicates segmentation of infrastructure between customers, based on purpose

17

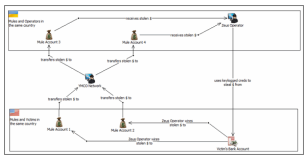
Avalanche botnet based hosting



18

Other identified services

- Other operations utilizing Avalanche botnet based infrastructure include a continuing eCrime enterprise specializing in money laundering operations
- Underground customers of Zeus service for July 2011 mobile incident likely also leveraging this money laundering service



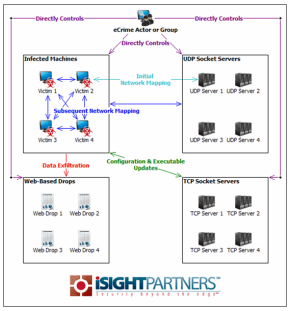
19

Service linked to new Zeus variants and versions

- In August 2011, service operators introduced new build variant 2.3.2.0
- In September 2011 a new, heavily modified Zeus version was observed in connection with this service's malware distribution infrastructure
  - Version utilizes a unique peer to peer command, control and communications architecture

20

Peer to peer Zeus architecture



21

Implications and Outlook

- While mobile threats represent an emerging concern, adversary operators are leveraging current infrastructure in new ways to impact a novel victim population
  - In September 2011, SpyEye in the mobile (SPITMO) variants identified, similar to ZITMO TTP
- Much of this infrastructure is acquired through transactions between continuing eCrime enterprises offering specialized services
- Identification and characterization of transactional services in the eCrime underground can provide insight to support countermeasures development, and warning of future threats

22

Case Study Conclusions

- Understanding adversary cyber threat activity is an intensive analytic task, requiring sustained collection access, large scale data processing, good analytic tools, and rigorous analytic tradecraft
  - The rapidly evolving nature of the mobile mission space places new emphasis on these requirements
- Robust visualization is a key requirement of these analytic approaches

23

Polling Question #2

- What describes your role?
  - Fraud investigator
  - Criminal investigator
  - Information technology / information security / information assurance
  - Management

24

Paul Henry

- vNet Security, LLC
  - Security, Incident Response and Forensics
- Board VP Florida Association of Computer Crime Investigators
- Board Member Ashlar Foundation – Security Industry Association
- Retained Security & Forensic Analyst @Lumension
- Member Miami Electronic Task Force
- Member HTCIA & HTCC
- Certified MCP+I, MCSE, CCSA, CCSE, CISSP-ISSAP, CISM, CISA, CIFI, CCE, ACE, GCFA, VCP
- Published author with 18+ book chapters and hundreds of articles in trade journals
- SANS Certified Instructor teaching Computer Forensics, Information Security and Risk Management

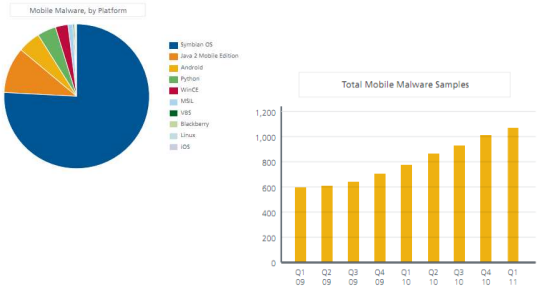
25

Practical Malware Threats

If I can download it and execute it… it is no longer a theoretical threat…. all that is lacking is the will to do it

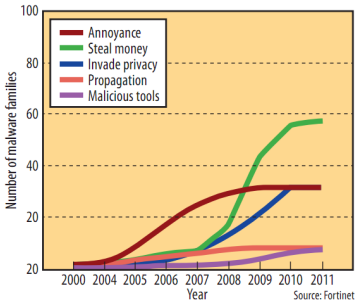
26

Mobile Malware Stats



27

Same Old Song & Dance



28

Apple iPhone & iPad Risks

- In many respects risk is in part about popularity
- Lets look at a few of the Apple sales stats
  - 250 Million iPods 2001 – 2010
  - iPhone and iPod Touch 40 Million + Worldwide
  - Well over 150,000 Applications existed in 2010 with an average of 250 added each day. Over 400,000 are expected by the end of 2011. Average application price is $2.90
  - Over 70% of the Fortune 100 deploy iPhones
  - 40% of users have incomes above $100k
  - If your not already working on Apple iPhone and iPad products you certainly will be……

29

Apple iPhone & iPad Risks

- Apple must review and approve each and every application
- Many users don't like to be told what they can do with the product and have chosen to Jail Break it
- That is what hackers are taking advantage of – a Jail Broken Apple product faces formidable malware challenges

JailbreakMe
Jailbreak to get tweaks and apps Apple won't allow in the App Store. Free, legal, safe.
You should sync with iTunes before using this tool.
More Info »

30

Apple iPhone & iPad Risks

- Just like our desktops and servers, Mobile Malware across all platforms will only get worse
  - Incident Response plans must now include Mobile Devices

Worm author tells media he initially infected 100 iPhones

31

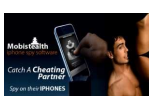
Apple iPhone & iPad Risks

- Remote monitoring of an iPhone is getting more common
  - In my forensics practice I see Spyware installed on iPhone's that is typically installed by a spouse but occasionally is installed by a coworker, disgruntled employee or a competitor

32

Apple iPhone & iPad Risks

- State laws vary but in many, all parties using the device must be notified if they are being monitored. Some actually collect data on the wire and may be considered to be wire tap issues….



33

Apple iPhone & iPad?

- Where has the iPhone (and the suspect) been – location data
  - Yes Apple patched it but the patch simply encrypts the data and limits it to 7 days of data stored on the phone

34

Android OS Based Devices

- Fastest growing mobile OS
- Over 300,000 Android activations a day
- Android overtook iOS as the dominant OS in US during 2H 2010
- First phone launched HTC G1 in 2008
- Currently an OS of choice for Motorola, HTC, Samsung, Sony Ericsson, among others

35

Android Device Risks

- With all of the news about malicious Droid Apps downloaded from the Droid Marketplace it is clearly apparent that testing apps is not a high priority before turning them loose on users

36

Android Device Risks

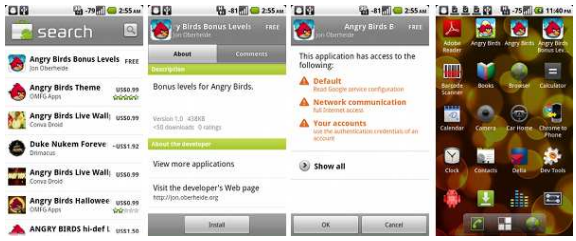
- A good example of Android security issues was highlighted with Angry Birds. Duo Security showed us that it was possible to install an app that allowed the unprompted installation of arbitrary applications with arbitrary permissions on a victim's device

http://blog.duosecurity.com

37

When Angry Birds Attack (1)

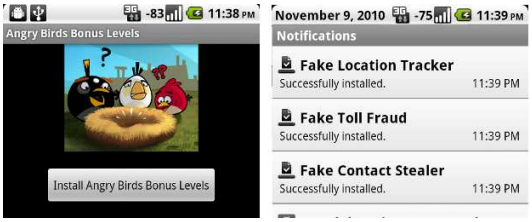
- Hmmmm…



38

When Angry Birds Attack (2)

- Ouch…



39

The Droid Dream Fiasco

- There are serious issues over at Google's Android Market

Over 50 "DroidDream" Malware Apps Removed from Android Market

By Sarah Perez / March 2, 2011 7:20 AM / 6 Comments

Tweet 273 Recommend 67 Hacker News Share & Save

Over 50 applications found to contain malware were removed from the Android Market yesterday, after being downloaded approximately 50,000 times. The apps contained a type of malware called "DroidDream," which was able to use exploit code to root (take administrative control over) the phones where it was installed and steal sensitive data from the devices. In addition, a second APK (an Android application file) was also found hidden inside the code, which could steal additional data.

40

It Is Poised To Get Worse…

- If you use an Android smartphone you are now 2.5 times more likely to encounter malware (malicious software) than you were six months ago.
- This year, 30% of Android users are likely to encounter a Web-based threat such as phishing scams, "drive by downloads" and browser exploits.

http://www.cnn.com/2011/TECH/mobile/08/04/lookout.threat.report.gahran/

41

Is the Droid Enterprise Ready?

- This raises concerns that Google's mechanisms for protecting Android users from threats simply aren't good enough at the present time
- While it's commendable that Google jumped quickly when a researcher notified them of the threat, that is simply not enough
- My personal opinion: With the risk of malicious apps "unchecked" in the Android Market I feel that the Droid may be a high risk if used within the enterprise…

42

iPhone Overview

- Each application runs in its own sandbox
  - Using Address Space Layout Randomization (ASLR) and Data Execution Protection (DEP)
  - Isolates data-store and memory
- Multitasking is limited to:
  - Background audio
  - VoIP
  - Background location
  - Push / Local notifications
  - Finish task started by user
- Every application must be signed (revocable)

43

iPhone Security Capabilities (1)

- Device protection
  - Strong passcodes
  - Passcode expiration
  - Passcode reuse history
  - Maximum failed attempts
  - Over-the-air passcode enforcement
  - Progressive device protection

44

iPhone Security Capabilities (2)

- Data protection
  - Remote and local wipe
  - Encrypted configuration profiles
  - Encrypted iTunes backups
  - Hardware encryption
- Network security
  - Cisco IPSec, L2TP, PPTP VPN protocols
  - SSL/TLS with X.509 certificates
  - WPA/WPA2 Enterprise with 802.1X
  - Certificate-based authentication
  - RSA SecurID, CRYPTOCard

45

iPhone Security Capabilities (3)

- Platform security
  - Runtime protection
  - Mandatory code signing
  - Keychain services
  - Common Crypto APIs
- Several vendors work with Apple's Mobile Device Management (MDM) framework that allows third party software to manage IOS devices
  - Good, Airwatch, MaaS360, McAfee EMM and MobileIron just to name a few…

46

High Level Best Practices (1)

- Update firmware to latest version
  - The most secure version of any software is normally the most current version
- Require a passcode
  - Go with the complex passcode
- Set auto-lock timeout and disable grace period for lock
- Erase data upon excessive passcode failures
- Enable data protection
  - This encrypts the data on the iPhone with IOS 4
- Turn off ask to join Networks

47

High Level Best Practices (2)

- Use an IPSEC VPN or SSL VPN
- Turn Off Bluetooth when not needed
- Enable forget WiFi networks
- Encrypt backups to iTunes
- Enable remote wipe capability
- Use the "Find My Phone App"
- Be sure to wipe / erase all data before return for service or recycling

48

Configuration Profiles

- Apple offers an iPhone Configuration Utility that can be used to create Configuration Profiles (or use third party product)
  - Mac
    - http://support.apple.com/kb/DL851
  - Windows
    - http://support.apple.com/kb/DL926
- Configuration Profiles can be deployed via a web server, over USB to the device, via MDM or via email (attachment)

49

Apple Resources

Enterprise

iOS 4 Enterprise Deployment Resources
How to integrate iOS 4 devices with your enterprise systems, including mail, calendaring and VPN. How to create and distribute custom configuration profiles and applications.

iOS 3 Enterprise Deployment Guide
How to integrate iOS 3 devices with your enterprise systems.

iPhone Support Communities – Enterprise
Discuss this topic with fellow iPhone users.

Downloads

iPhone Configuration Utility for Mac OS X
iPhone Configuration Utility lets you easily create, maintain, encrypt, and push configuration profiles, track and install provisioning profiles and authorized applications, and capture device information including console logs.

iPhone Configuration Utility for Windows
iPhone Configuration Utility lets you easily create, maintain, encrypt, and install configuration profiles, track and install provisioning profiles and authorized applications, and capture device information including console logs.

50

Suggested Policy Details (1)

- Passcode
  - Require passcode on the device = enabled
  - Require alphanumeric value = enabled
  - Minimum passcode length = 8
  - Minimum number of complex characters = 2
  - Maximum passcode age = 60 days
  - Auto-Lock = 5 minutes
  - Passcode history = 5
  - Grace period of device lock = 1 minute
  - Maximum number of failed attempts = 7

51

Suggested Policy Details (2)

- Restrictions
  - Allow screen capture = disabled
  - Force encrypted backups = enabled
  - Allow use of Safari
  - Enable autofill = disabled
  - Force fraud warning = enabled
  - Enable JavaScript = enabled
  - Block pop-ups = enabled
  - Accept cookies = From visited sites

52

Suggested Policy Details (3)

- Wi-Fi -> set as required
- VPN -> set as required
- Email -> as required
  - enable Use SSL whenever possible for incoming and outgoing
- Exchange ActiveSync
  - Use SSL = enabled
  - Include Authentication Credential Passphrase = disabled
- LDAP
  - Use SSL = enabled

53

Suggested Policy Details (4)

- CalDAV
  - Use SSL = enabled
- CardDAV
  - Use SSL = enabled
- Subscribed Calendars
  - Use SSL = enabled
- Web Clips -> set as required
- Credentials -> set as required for NAC and VPN access
- SCEP -> set as required

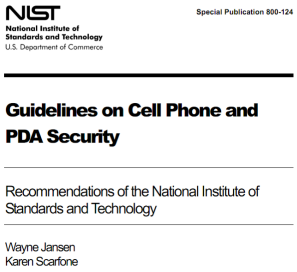
54

Suggested Policy Details (5)

- Mobile Device Management -> set as required
- Advanced -> set as required

55

Other Resources


NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-124

Guidelines on Cell Phone and PDA Security

Recommendations of the National Institute of Standards and Technology

Wayne Jansen
Karen Scarfone

http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf

56

MDM using Active Sync (1)

- Connects directly to enterprise mail servers like Microsoft Exchange and Lotus Domino via Exchange ActiveSync providing users push email, calendar events, and contacts.
- IT can enforce complex passcodes and remotely wipe a lost or stolen iPhone instantly.
- Certificate-based authentication means only approved users get access to Exchange and encrypted SSL communication to and from the server keeps data safe.

57

MDM using Active Sync (2)

- Check to ensure port 443 is open on the firewall. If your company allows Outlook Web
  - Port 443 is most likely already open.
- On the Front-End Server, verify that a server certificate is installed and enable SSL for the Exchange ActiveSync virtual directory in IIS.
- If you're using a Microsoft Internet Security and Acceleration (ISA) Server, verify that a server certificate is installed and update the public DNS to resolve incoming connections.

58

MDM using Active Sync (3)

- Make sure the DNS for your network returns a single, externally routable address to the Exchange ActiveSync server for both intranet and Internet clients. This is required so the device can use the same IP address for communicating with the server when both types of connections are active
- If you're using a Microsoft ISA Server, create a web listener as well as an Exchange web client access publishing rule. See Microsoft's documentation for details.

59

MDM using Active Sync (4)

- For all firewalls and network appliances, set the Idle Session Timeout to 30 minutes. For information about heartbeat and timeout intervals, refer to the Microsoft Exchange documentation at:
  - http://technet.microsoft.com/en-us/library/cc182270.aspx
- Configure mobile features, policies, and device security settings using the Exchange System Manager. For Exchange Server 2007 and 2010, this is done in the Exchange Management Console.

60

MDM using Active Sync (5)

- Download and install the Microsoft Exchange ActiveSync Mobile Administration Web Tool, which is necessary to initiate a remote wipe. For Exchange Server 2007 and 2010, remote wipe can also be initiated using Outlook Web Access or the Exchange Management Console.

61

MDM using Active Sync (6)

- Basic authentication (username and password)
  - Enable Exchange ActiveSync for specific users or groups using the Active Directory service. These are enabled by default for all mobile devices at the organizational level in Exchange Server 2003, 2007, and 2010. For Exchange Server 2007 and 2010

62

MDM using Active Sync (7)

  - By default, Exchange ActiveSync is configured for basic user authentication. It's recommended that you enable SSL for basic authentication to ensure credentials are encrypted during authentication.
- Certificate-based authentication
  - Install enterprise certificate services on a member server or domain controller in your domain (this will be your certificate authority server).
- Configure IIS on your Exchange front-end server or Client Access Server to accept certificate-based authentication for the Exchange ActiveSync virtual directory.

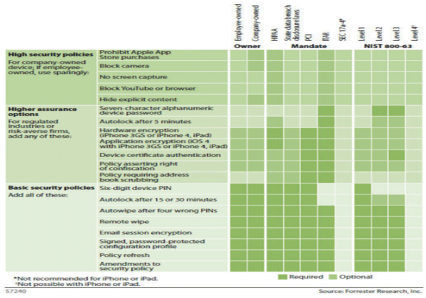
63

MDM using Active Sync (8)

- To allow or require certificates for all users, turn off “Basic authentication” and select either “Accept client certificates” or “Require client certificates.”
- Generate client certificates using your certificate authority server. Export the public key and configure IIS to use this key. Export the private key and use a Configuration Profile to deliver this key to iPhone. Certificate-based authentication can only be configured using a Configuration Profile.

64

Mandates and Standards



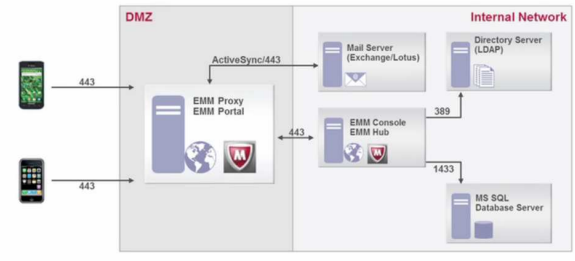
65

Third Party MDM Products

- Enterprise Mobility Management
  - It’s From McAfee
    - So yes it integrates with ePO
  - Easy setup and it does not require that the users environment be using Exchange
  - Offers “Selective Wipe” capabilities vs. wiping the entire device
  - Manages multiple devices by group not just individually
  - Allows Apps to be installed via the management interface while disabling in App purchases
    - More secure control of application installation

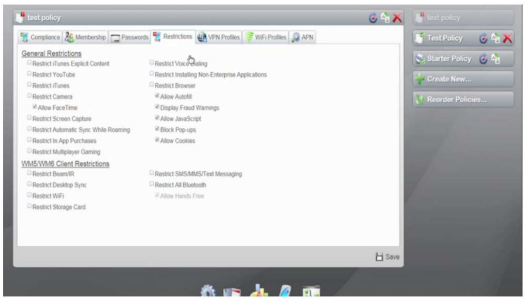
66

EMM Architecture



67

EMM Policy Management

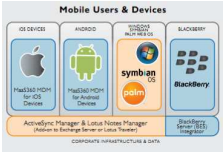


68

EMM Provisioning

69

Getting Good Reviews…



MaaS360 by Fiberlink

MaaS360® Mobile Device Management

70

MDM Is Hot – Lots Of Players

NOTIFY TECHNOLOGY Mobile Device Management

71

iPhone and Android
Incident Response & Forensic
Consideration

Why you really need to worry about employees losing their mobile devices!

72

Apple iPhone IR & Forensics (1)

- A treasure trove of information is stored in the iPhone and iPad
  - For starters:
    - User accounts
    - Contacts
    - Call history
    - SMS Messages
    - Messages Google Mail and Yahoo! Messenger
    - Skype Chat
    - History of Google Maps, stored in iPhone and iPad
    - Dynamic Dictionary
    - Automatic Screen Shots
    - Most apps store data so the list simply goes on and on and on

73

Is a Logical Analysis Enough? (1)

- For many a logical image that represents the logical file system as it appears to the operating system and it's analysis is sufficient.

74

Is a Logical Analysis Enough? (2)

- Some information is maintained in databases on the iPhone and when deleted actually still exists but is simply marked in the database as deleted

75

Is A Logical Analysis Enough? (3)

- No longer seen by the user in the applications GUI hence some “deleted” information can in fact be recovered in a logical extraction.

- So yes a logical analysis may provide a significant amount of data but… it is of course not equivalent to a physical analysis, more about that in a few minutes

76

What is a Physical Analysis?

- For starters a Physical image is a bit by bit copy of the entire physical data store including that which is outside of the operating systems view of the storage media’s file structure.
  - A typical physical analysis can then carve files from both allocated and unallocated space

77

Now let's get Physical

- Significantly more data is typically found with a physical image such as deleted files including images and other user data that effectively needs to be carved from the physical image (includes all storage media both allocated and unallocated space including that which is outside the scope of the file system) just like on a PC or server hard disk.

78

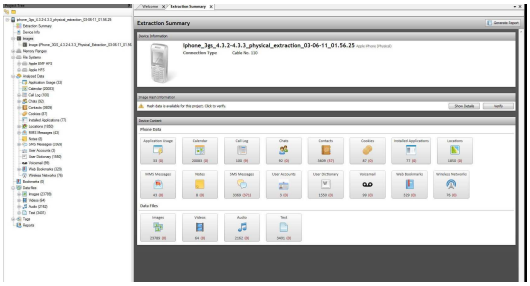
Physical Analysis iPhone

UFED iPhone Physical
Preparing your device for extraction
Successfully entered DFU Mode.
You can release the Home button now
The wizard is now uploading the forensic program to the device. This will take a minute.
Waiting for device to boot in Forensic Mode
Step 17 / 17
Total Progress: 92%

Now provides “On The Fly Decryption !

79

Physical Analysis ROCKS!



80

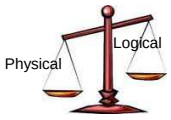
Logical vs. Physical (1)

- What did I get in my Physical Analysis vs. Logical Analysis
  - Additional evidence recovered included:
    - 22,000+ images
    - 59 videos
    - 1000+ audio files
    - 16,000+ locations
    - 60+ chats (included Facebook and Skype)
    - 30+ MMS
    - 3300+ text files
    - 36 Mac Mail Emails
    - 22 Gmail Emails
- Python Scripts to carve data are a big differentiator in Mobile device forensics!

81

Logical vs. Physical (2)

- Doing a logical analysis you have to consider that you are really only getting part of the evidence. Simply put in my opinion a thorough analysis requires a physical extraction and its more complete examination…



82

Final Thoughts on Forensics

- Mobile Phone Forensics is not for everyone as it is an expensive undertaking to be able to cover the many phones in use today
  - I have done everything from throw away Samsung's, Blackberry's, Droids, iPhones and iPads without issue
- Apple (and everyone else) constantly makes changes that literally break any tool used to analyze their products i.e. the mandatory encryption in iPhone 4.x
- Physical Analysis is the future of Mobile Device Forensics

83

But Wait, what about the iPad

- In the simplest of terms it is basically the same OS so you literally have the same capabilities
  - I have achieved similar results in my forensics practice analyzing Apple iPads

84

Android IR & Forensics

- A treasure trove of evidence is stored in an Android
- Logical analysis can provide:
  - Browser history, Call Logs, Contact Methods, External Image Media (meta data), External Image Thumbnail Media (meta data), External Media, Audio, and Misc. (meta data), External Videos (meta data), MMS, MMS Parts (includes full images sent via MMS), Organizations, People, SMS, List of all applications installed and version, Contacts – Extensions, Groups, Phones, Settings

85

In Closing (1)

- With respect to the risk of malicious applications; The process that delivers an unmatched security advantage to Apple is also what users seem to despise the most…
  - The closed nature of the Apple products
- Remember that an "out of the box" unsecured Mobile Devise represents a significant risk to the enterprise
  - i.e. Blackberry, Android, iPhone or iPad

86

In Closing (2)

- Notable risk mitigation can be achieved by following a few simple best practices
- For those iPhone and iPad enterprise users with Microsoft Exchange or Lotus Domino via Exchange additional risk mitigation is available via MDM using Microsoft Active Sync
  - Not using Exchange ? Use the Apple Configuration Utility or one of the other third party MDM solutions mentioned

87

Polling Question #3

- Has your organization been impacted by incidents involving malware infection of mobile devices?
  - Yes, frequently
  - Yes, in individual cases
  - No, to date no incidents detected
  - No, confident controls are in place to prevent infection
  - No, my organization may lack capabilities to detect incidents

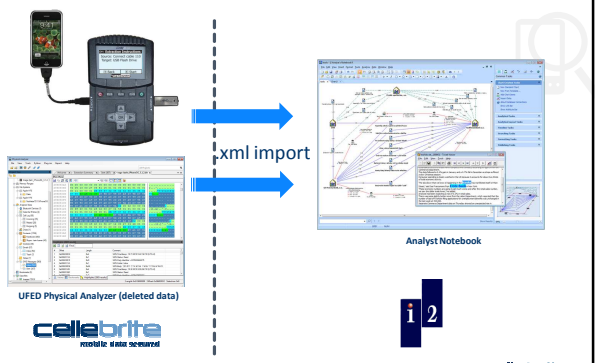
88

Christopher Shin

- Chris Shin is the VP Engineering for Cellebrite USA Corp since 2002
- Chris has 12+ years experience in the mobile communications industry, specializing in mobile devices and forward looking technologies.
- Mr. Shin's experience includes acting as a liaison for all US-based carrier customers and managing multiple technical engineering projects with device original equipment manufacturers and original design manufacturers.
- Previous to Cellebrite, Mr. Shin acted a Member of Technical Staff at Verizon Wireless HQ, in Warren NJ.
- Chris holds a Bachelor of Science degree from Rutgers College of Engineering, NJ in the fields of Electrical and Computer Engineering.

89

Seamless Integration of UFED Output into i2 Analyst Notebook



90

All rights reserved © 2011, Cellebrite

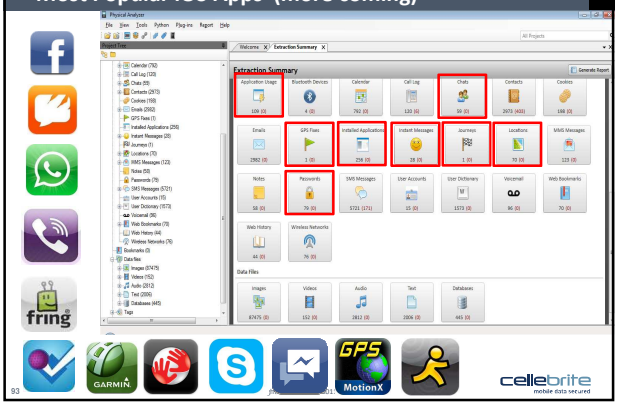
Unmatched iOS Support: Latest Enhancements

Latest feature functionality enhancements include:

- User Password extraction (even locked devices)
- Real Time decryption of iOS 4 File System
- Keychain decryption allows access to **passwords to email, WiFi and other application accounts**
- **Facebook Messenger** and **TigerText** apps (real time decryption) added to the growing library of apps able to be decoded by Physical Analyzer
- Integrated SQLite browser for viewing of iPhone database files
- iOS 5 support

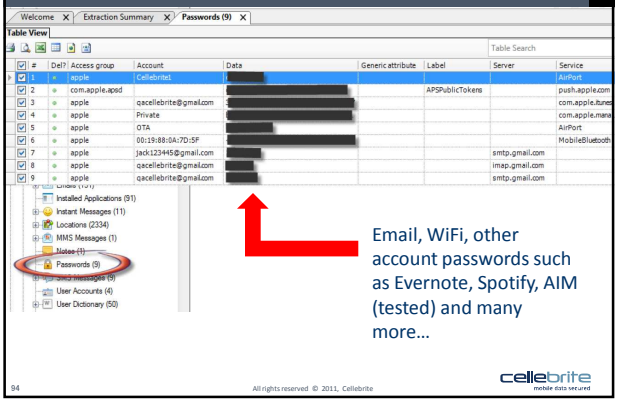
92 All rights reserved © 2011, Cellebrite cellebrite mobile data secured

Physical Analyzer: Automated Decoding of the Most Popular iOS Apps (more coming)



93 cellebrite mobile data secured

iPhone Keychain Decryption



Email, WiFi, other account passwords such as Evernote, Spotify, AIM (tested) and many more…

All rights reserved © 2011, Cellebrite

Android Physical (Pattern Lock Extraction)

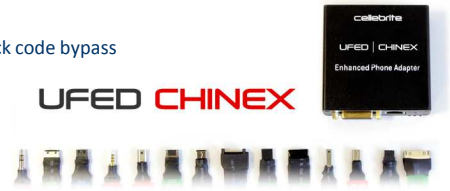
Android Physical Highlights

- 15+ devices currently able to be extracted, **even while locked** (unique to Cellebrite)
- **50+** devices for physical extraction in next release
- Proprietary bootloaders developed by Cellebrite
- File System (extX, YAFFS2) and database decoding in Physical Analyzer
- Android Apps decoding - coming soon
- Samsung Galaxy devices (S, S2, Tablet) coming soon with lock bypass functionality

All rights reserved © 2011, Cellebrite

CHINEX: Physical Support for Thousands of Generic Chinese Handsets ("Knock-offs")

- Physical extraction and decoding of live and deleted data for thousands of Chinese mobile phones, including dual SIM models and knock-offs emerging in markets everywhere
- Extraction based on Cellebrite's proprietary **read only** boot loaders ensuring a forensically sound process
- Lock code bypass



All rights reserved © 2011, Cellebrite

i2 / Cellebrite Video

Company

Founded: 1990
Headcount: 400
Headquarters Locations:
-Americas: McLean, VA
- Vancouver, CA
- EMEA: Cambridge, UK
- AsiaPac : Canberra, AU

Clients

- 350,000 users
- 4500 organizations
- 150 countries

Products

- COPLINK Product Line
- Analysis Product Line

i2 Cyber attribution

- Know **where**, **when**, **why**, **how** and by **whom** your network is being compromised
- Understand threats and their consequences
- Develop tactical intelligence
  - Discover hostile IP and DNS information – "cyber addresses"
  - Define attacker methodology
  - Globally map attackers and threats
- **Post-attribution remediation**
  - Define and address vulnerabilities
  - Harden defenses
  - Target attackers

100

Benefits of attribution and remediation

Reduce exfiltration of sensitive data

Prevent financial theft

Prevent disruption of operations

Eliminate compromises that lead to more serious attacks

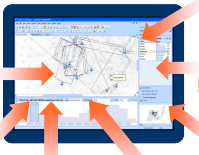
Reduce risk and liability
Improve compliance

101

i2 Cyber: What does it look like?

Analyst's Workstation

- Analyst's Notebook
- Dataminer
- GIS Interfaces



Un-structured text,email & HTML

TextChart

Custom-built Connectors

All Source Data

3rd Party Tools Applications

i2 SDK

iBase

Analyst's Notebook

i2 Cyber IP/DNS Resolution 8.5

- IP to DNS and DNS to IP Resolution
- Geo-locate country and LAT / LONG
- Spam blacklist checker
- Regular bulk updating of threat data

102

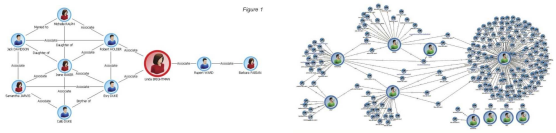
i2 Cyber – How can it help me?

- Central analytical environment means key relationships and connections are not missed
- "Natively Wired" to all data sources and GIS capability
- Reduces quantity and improve quality of information
- Leverages cyber data with other real-world sources…"connecting the cyber world with the real world"
- SNA mapping shows how and where to disrupt attack networks
- Acquire and analyze data from social networks to gain intelligence on internal and external fraud and threats
- Access intelligence on individuals and groups that may pose a threat to your facilities or personnel
- Acquire and analyze data that can help to reduce brand and reputational fraud
- Unites and enhances – does not replace – your existing infrastructure
- Automate manual and time consuming analysis tasks

103

i2 Social Network Analysis

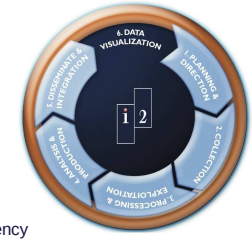
- Visual and mathematical analyses of complex human and computer networks
- Discover sources and distribution of power: Who knows whom; who does business with whom; and who wields greatest power
- See how communications flow in networks and sub-networks
- Monitor patterns between communications nodes, performance and key goals
- Combines data extraction, manipulation, analysis and visualization
- Centrality, Betweeness, Closeness, Degree, Eigenvector, Link Direction and Weight



104

Use i2 Cyber investigative results to…

- Learn from attacks
- Discover your network vulnerabilities
- Harden your defensive perimeter
- Track Advanced Persistent Threats (APTs)



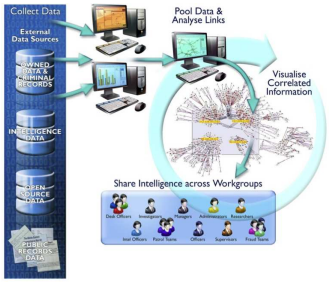
…Leading to:

- Improved performance and efficiency
- Elimination of manual and repetitive tasks
- Enterprise level awareness

105

Share Intel & Analysis

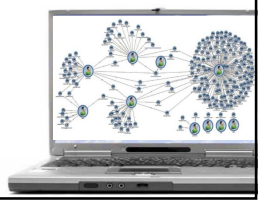
- Extend the reach of your intelligence and analysis through the cloud
- Place real time intelligence at point of need
- Facilitate operational team collaboration
  - Mangers, investigators, supervisors
  - Researchers, intelligence officers, fraud teams



106

Present & communicate intelligence

- Enable faster and more informed decision making
- Clearly communicate threats and impacts with comprehensive and concise visualization
- All visualization is 100% data-driven
- Package cases for law enforcement



Q&A

- Please submit your questions via the online dashboard
- Any questions that we cannot get to today, we will follow up on individually

108

Contact Our Speakers

Joshua Work
Chief Intelligence Analyst
jwork@isightpartners.com

Paul Henry
vNet Security
phenry@vnetsecurity.com

Christopher Shin
VP Engineering, Cellebrite USA
christopher@cellebriteusa.com

Brandt Heatherington
Global Director, i2 Group
Brandt.heatherington@i2group.com

109

Get the Free Whitepaper!

Contact us for more information
and to receive the white paper
5 Emerging Mobile Cyber Crime Trends
sales.americas@i2group.com
888-546-5242
salesinfo.emea@i2group.com
+44 (0) 1223 728660

The whitepaper is also available on the ACFE dashboard
for this event under “i2 Resources”

110

Thank You for Attending!

111